Overview of draft-ietf-sidr-arch-00.txt

Steve Kent

BBN Technologies

Architecture Document Goal

- Provides an overview of the proposed architecture
- Major elements of the architecture
- Underlying assumptions
- Role each element plays in the architecture
- How the elements work together
- References to other documents that provide details about elements of the architecture

Document Outline

- PKI
  - CA certificates
  - EE certificates
  - Trust anchors
- ROAs
  - Syntax & semantics
  - Revocation
- Repository system
  - Contents & structure
  - Access protocols
  - Access controls
- Common Operations
  - Certificate issuance
  - ROA management
  - Route filter construction

PKI

- All certificates are “resource certificates”
  - Attest to holdings of address space and/or AS numbers
- CA certificates
  - Every resource holder is a CA
  - Resource holders can have multiple certificates
- EE certificates
  - Used to verify non-PKI signed objects, e.g., ROAs
  - 1-1 correspondence with signed objects enables simple revocation
  - Single-use private key model improves security
- Trust anchors
  - Choice of a TA is up to each relying party, the RIRs (and IANA) are just the default TAs

Open Issues for PKI Section

- Add a discussion of CA certificates from multiple allocation sources
- Certificate name conventions (or put in certificate profile?)
- Other topics?

ROAs

- ROA definition
- ROA content discussion
- ROA syntax
- ROA semantics
- ROA revocation

Open Issues for ROA Section

- Add cites to ROA I-D for
  - Syntax
  - Semantics (e.g., ROA validation vs. EE certificates)
  - Revocation
- Need discussion of how to verify an advertisement covered by multiple ROAs
- Need discussion of how a ROA for a non-CIDR address range is matched against a prefix
- …

Repository System

- What is stored
  - Certificates
  - CRLs
  - Signed objects that all users require, e.g., ROAs
- Security considerations
  - Integrity of contents that are already signed
  - Availability
  - Need for access controls (but no spec for them)
- Repository operations
  - Upload
  - Download
  - Change/delete

Open Issues for Repository Section

- Need more discussion of repository access protocols (e.g., rsynch, others)
- Need to define repository access controls
- Need more discussion of repository structure (e.g., file naming convention, links, …)
- Need discussion of repository distribution model

Common Operations

- Certificate issuance
- CRL issuance
- ROA management
  - Ties to repository management (e.g., remove revoked ROAs and EE certificates from the repository system)
  - Single-homed subscribers
  - Multi-homed subscribers
  - Portable allocations
- Constructing route filters using ROAs

Open Issues for Operations Section

- Discuss certificate revocation and renewal, not just issuance
- Cite certificate profile I-D for certificate issuance, renewal, and revocation discussions
- Cite ROA I-D in ROA discussion
- Discuss how to match ROAs to BGP UPDATEs
- Add a discussion of how an ISP can use ROAs (or other PKI mechanisms) to verify that a subscriber is the holder of address space he wants the ISP to advertise

The Official SIDR Joke?

- A certificate, a CRL, and a ROA walk into an AS …